The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-*Puttaswamy* World

Vrinda Bhandari and Karan Lahiri*

Abstract

Indian law, as it stands, arms the State with disproportionate and unchecked power to extract and utilise private information. First, executive discretion to authorise and monitor surveillance is not subject to any independent inter-branch oversight. And second, illegally obtained evidence is usually admissible in courts as long as it is relevant. In this article, we examine the possible impact on this status quo flowing from the judgments of the Supreme Court of India in *KS Puttaswamy v Union of India*, dealing with the right to privacy, and *KS Puttaswamy v Union of India (II)*, dealing with the constitutional challenge to the centralised, biometric-based, unique identity scheme, commonly known as 'Aadhaar'. We unpack the doctrinal toolkit that these two judgments provide us with, including the standard of proportionality applied, and argue that they offer a framework for testing the existing system of laws governing surveillance. The thread running through our analysis is the judiciary's role in preserving the rule of law and providing a counterweight to the executive's power to deploy the State's surveillance infrastructure. By focusing on individual liberty as a counterweight to State power, we argue that there is

* The authors are Advocates practising before the Supreme Court of India. Vrinda read for the BCL and the MPP at Magdalen College, University of Oxford and Karan completed his LLM from Harvard Law School. They would like to thank Mr KV Viswanathan (Senior Advocate), Gautam Bhatia, Apar Gupta, Ramanjit Singh Chima, and N Sai Vinod, as the discussions surrounding *Internet Freedom Foundation & Anr v Union of India*, Writ Petition (C) No. 44/2019 have directly contributed to the portions of this article which deal with the aspect of judicial oversight. The authors are also grateful to Dr Aparna Chandra, who provided the authors with an early manuscript of her article titled 'Proportionality in India: A Bridge to Nowhere?' (2020) 3(2) U of OxHRH J 55. The authors would also like to thank the editorial team at the Oxford Human Rights Hub Journal for their thoughtful comments.

now a starting point for insisting on judicial oversight of surveillance action and exclusion of illegally obtained evidence

Keywords: Privacy; Surveillance; Illegally Obtained Evidence; Exclusionary Rule; *Puttaswamy*; *Aadhaar*

1. Introduction

The Surveillance State is at our doorstep. We live in an age of big data, where technology has enabled governments to monitor the lives of its citizens more easily and at diminishing cost.[1] This is being done in a variety of ways, including wiretapping; video-graphing; geolocation tracking; data mining; intercepting, decryption and monitoring of emails; and, tracking internet and social media usage.[2] Surveillance today is now both wider, covering a larger section of society, and deeper, being more invasive.[3]

The silent shadow of surveillance in India grows more ominous not only because the government is expanding its technological capacity to watch citizens, but also because of the lack of transparency and accountability.[4] In ongoing litigation before the Supreme Court of India, the Indian government revealed that it had been undertaking electronic surveillance on the basis of a 'Standard Operating Procedure', [5] a

[1] Zachary Smith, 'Privacy and Security Post Snowden: Surveillance Law and Policy in the United States and India' (2014) 9 Intercultural Human Rights Law Review 137, 192-95, 197; Ronald Krotoszynski Jr, *Privacy Revisited* (OUP 2016) 169-71, 181-82, 186.

[2] Robyn Greene, 'How the Government Can Read Your Email' (*Politico,* 22 June 2017) <https://www.politico.com/agenda/story/2017/06/22/section-702-surveillance-program-national-security-000463> accessed 29 May 2019; Jennifer Valentino-DeVries, 'Tracking Phones, Google Is a Dragnet for the Police' *The New York Times* (New York, 13 April 2019) <https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html> accessed 29 May 2019.

[3] Sarah Brayne, 'Big Data Surveillance: The Case of Policing' (2017) 82(5) American Sociological Review 977, 979.

[4] Chaitanya Ramachandran, '*PUCL v. Union of India* Revisited: Why India's Surveillance Law Must Be Revised for the Digital Age' (2014) 7 National University of Juridical Sciences Law Review 105, 112-14, 117; Vipul Kharbanda, 'Policy Paper on Surveillance in India' (*The Centre for Internet & Society*, 3 August 2015) <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india> accessed 25 May 2019; Rishabh Bailey, Vrinda Bhandari, Smriti Parsheera and Faiza Rahman, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' (*NIPFP Macro/Finance Group*, 1 August 2018) <http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed 22 May 2019.

[5] 'Centre Defends Snooping Notification in the Supreme Court' (*The Leaflet,* 11 March 2019) <https://theleaflet.in/centre-defends-snooping-notification-in-the-supreme-court/> accessed 26 May 2019.

document which was not previously in the public domain. This has given rise to fears of increased centralisation of power in the hands of the executive, with surveillance operations being cloaked in secrecy.[6]

The law as it stands falls far short of ensuring accountability. First, the statutory pre-conditions for valid surveillance are widely worded,[7] allowing the government ample scope to justify the legality of individual instances of surveillance. Second, in India, the discretion to authorise and monitor surveillance operations has been vested entirely in the executive. These decisions are not subject to any independent inter-branch oversight, either by the parliament or by the judiciary; nor is there any requirement for hearing the affected individual before or after making the decision to place them under surveillance.[8] Third, under Indian law, illegally obtained evidence is usually admissible in courts as long as it is relevant.[9]

The upshot of this, particularly the last two elements—exclusive executive control over surveillance authorisation and admitting illegally obtained evidence during trial—gives the State disproportionate and unchecked power to extract and utilise private information.

In this article, however, we push back against this status quo, and examine the possible impact of the judgments of the Supreme Court of

---

[6] 'Secret Operating Procedure for Digital Snooping Revealed. Confirms Fears of Centralisation of Executive Power, Zero Judicial Scrutiny and Oversight' (*Internet Freedom Foundation*, 11 March 2019) <https://internetfreedom.in/revealed-secret-operating-procedure-followed-by-the-govt-for-digital-snooping/> accessed 26 May 2019.

[7] Telephone tapping is carried out under Section 5(2) of the Indian Telegraph Act 1885 and may be ordered on the 'occurrence of any public emergency' or 'in the interest of the public safety'. Section 69 of the Information Technology Act 2000 ('IT Act'), which pertains to online surveillance, throws the net even wider, allowing the Central Government or State Governments to authorise an agency to 'intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource' if it is 'in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence'. Conceptually, therefore, the statute allows online surveillance even for investigating the pettiest of crimes. The provision additionally requires internet service providers 'extend all facilities and technical assistance' to the intercepting agency. Therefore, the statute itself does little to limit the powers of the State. See also Vrinda Bhandari and Renuka Sane, 'Towards a Privacy Framework for India in the Age of the Internet' (2016) NIPFP Working Paper No 179, 13-14 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2892368> accessed 05 June 2019.

[8] See (n 73) and (n 74).

[9] *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600 [154]-[155]; *Umesh Kumar v State of Andhra Pradesh* (2013) 10 SCC 591 [35]. See Talha Rahman, 'Fruits of the Poisoned Tree: Should illegally obtained evidence be admissible?' (2011) Practical Lawyer April S-38 <http://www.supremecourtcases.com/index2.php?option=com_content&itemid=5&do_pdf=1&id=20972> accessed 29 May 2019.

India in *KS Puttaswamy v Union of India*[10] (*Puttaswamy*) and *KS Puttaswamy v Union of India (II)*[11] (*Aadhaar*) on the status quo. We first unpack the doctrinal toolkit that these two judgments provide us with. We then use this as a starting point to re-examine the current standard of admitting illegally obtained evidence, and to test whether judicial oversight is a minimum requirement for surveillance provisions to remain constitutionally valid. At the heart of both questions lies the common theme of the judiciary's role in preserving the rule of law and providing a counterweight to the executive's power to deploy the State's surveillance infrastructure.

To narrow the scope of our inquiry, we define illegally obtained evidence as being limited to reliable and relevant evidence obtained by a government authority through surveillance carried out in violation of the right to privacy. To be clear, surveillance actions conducted in violation of statutory provisions, namely the Indian Telegraph Act 1885 and Information Technology Act 2000, automatically trigger a privacy violation.[12]

Section 2 deals with two important changes in the privacy landscape, introduced by *Puttaswamy* and *Aadhaar*, directly relevant to surveillance. Section 3 uses the framework provided by these two decisions to understand whether and to what extent judicial oversight over surveillance is a necessary safeguard mandated by the Indian Constitution. Section 4 looks at whether these two rulings can be used to introduce an exclusionary rule in India, applied to evidence collected through illegal surveillance in violation of the right to privacy. Section 5 concludes.

2. *Privacy and Surveillance After* Puttaswamy

The Indian government established a centralised biometric and demographic database of its residents under the Aadhaar Scheme. The constitutionality of the Aadhaar Scheme was challenged before the Supreme Court in 2012. During one of the hearings in 2015, the government took the position that there was no fundamental right to privacy under the Constitution.[13] The Attorney General argued that although the Supreme Court had previously alluded to the existence of a

[10] (2017) 10 SCC 1.
[11] (2019) 1 SCC 1.
[12] *PUCL v Union of India* (1997) 1 SCC 301 [17];*Dnyaneshwar v State of Maharashtra* (2019) SCC Online Bom 4949 [18].
[13] *Puttaswamy* (n 10) [4]-[6].

right to privacy in a number of cases,[14] these pro-privacy pronouncements conflicted with earlier decisions handed down by larger benches of the Supreme Court in *MP Sharma v Satish Chandra*[15] and *Kharak Singh v State of UP*[16] Consequently, a nine-judge bench of the Supreme Court came together to decide whether the right to privacy was, in fact, a protected right under the Indian Constitution in *Puttaswamy*.

In this seminal decision , the Court unanimously held that the right to privacy was an 'intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution'.[17] It also overruled *MP Sharma* and *Kharak Singh*, to the extent that they held that the right to privacy was not protected by the Constitution.[18] The striking down of these cases in *Puttaswamy* is significant in mapping the trajectory of the law relating to privacy and surveillance in India. Subsequently, a five-judge bench of the Supreme Court in *Aadhaar* weighed the Aadhaar Scheme against the right to privacy and largely upheld the constitutionality of the Scheme (or by its full name, the Targeted Delivery of Financial and Other Subsidies, Benefits, and Services Act 2016) while striking down certain provisions.[19]

Puttaswamy and *Aadhaar* changed the legal landscape in India in at least two distinct ways. First, they explicitly recognised the harms of surveillance, especially in the digital age. Second, while building upon an existing foundation, they crafted a tiered proportionality test applicable in a fundamental rights challenge.

A. The Privacy Harms of Surveillance

The very existence of a State surveillance apparatus, regardless of its actual use, impinges upon personal liberty[20] and the freedom of speech and expression.[21] More than a mere negative right to be let alone,[22] privacy creates the conditions necessary for human intimacy,[23] while enabling the exchange of unpopular or unconventional ideas without fear of

[14] *Gobind v State of MP* (1975) 2 SCC 148; *R Rajagopal v State of TN* (1994) 6 SCC 632; *PUCL* (n 12).

[15] [1954] SCR 1077.

[16] [1964] 1 SCR 332.

[17] *Puttaswamy* (n 10) [652.1]-[652.4].

[18] ibid.

[19] *Aadhaar* (n 11). See Vrinda Bhandari and Renuka Sane, 'A Critique of the Aadhaar Legal Framework' (2019) 31(1) National Law School of India Review 72.

[20] Article 21 of Constitution of India 1950.

[21] Article 14 of Constitution of India 1950.

[22] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 193-95.

[23] Charles Fried, 'Privacy' (1968) 77 Yale Law Journal 475

opprobrium or consequence.[24] Equally, a Panopticon-like digital surveillance apparatus stultifies expression and openness, merely by virtue of the subject's knowledge that she is being watched.[25] Subba Rao J, in his dissent in *Kharak Singh*,[26] had explained how surveillance places psychological restraints that conditions our minds, and affects their freedom to think and express freely, in a way that impacts their personal liberty. While overruling *Kharak Singh*, the nine-judge bench in *Puttaswamy* recognised Subba Rao J's dissent as constitutionally correct.[27] Subba Rao J was prescient, because today the government has the means to listen in to our private conversations, read our private communications, and even track our every movement on a daily basis. We are less likely to exchange radical ideas or attend political meetings, for instance, if we know that the government may be privy to our exchanges and movements and anticipate retaliation for dissent.

Put another way, surveillance impacts the right to privacy, especially intellectual privacy, which is the freedom to develop ideas without being monitored;[28] and informational privacy, which incorporates the ideas of secrecy, control and anonymity.[29] The fear of intimate information being revealed about one's lifestyle and personal choices has an empirically demonstrable[30] chilling effect[31] on free speech and association, preventing/discouraging people from reading and exchanging unorthodox, unpopular, contentious or offensive ideas. In 2017, for the first time, these ideas were expressly incorporated by the *Puttaswamy* judgment into India's constitutional articulation of privacy.[32] In this way, *Puttaswamy* expanded the vocabulary available to Indian courts in dealing with cases of surveillance, by elaborating on the reasons for which privacy mattered and could be understood to be violated in cases of surveillance.

Given the power imbalance between the citizens and the State, there is a higher expectation of privacy as against the State, as compared to private

[24] ibid 483.

[25] Christopher Slobogin, 'Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity' (2002) 72 Mississippi Law Journal 213, 240-51.

[26] *Kharak Singh* (n 16).

[27] *Puttaswamy* (n 10) [17] [22] [24] (Chandrachud J), [341]-[344] (Chelameswar J), [446] [452] [475] (Nariman J); *Aadhaar* (n 11) [168].

[28] Neil Richards, 'Intellectual Privacy' (2008) 87 Texas Law Review 387, 389.

[29] *R v Spencer* (2014) 2 SCR 212 [38]-[47] (Canadian Supreme Court).

[30] Elizabeth Stoycheff, 'Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring' (2016) 93(2) Journalism & Mass Communications Quarterly 296; Alex Mathews and Catherine Tucker, 'Government Surveillance and Internet Search Behavior' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564> accessed 29 May 2019.

[31] C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (8 April 2014) [37] (Court of Justice of the EU).

[32] *Puttaswamy* (n 10) [146], [170], [214], [250] (Chandrachud J).

citizens. This is particularly due to the concentration of power in the hands of the State, their monopoly over violence, and the possibility of its misuse.[33] In India, these concerns are heightened since many law enforcement authorities such as the Central Bureau of Investigation (CBI), the Intelligence Bureau (IB), and the Research & Analysis Wing (R&AW), lack any statutory basis, and function with minimal accountability.[34] In this context, surveillance increases this State-citizen asymmetric power dynamic, which, as Richards points out, can lead to selective enforcement, discrimination and blackmail.[35] These dangers are intensified in the case of secret surveillance.

By acknowledging[36] the psychological restraints flowing from surveillance (as in the dissenting opinion in *Kharak Singh*), *Puttaswamy* implicitly recognises the dangers posed by the secret nature of State-surveillance, which ensures that individuals have no way of knowing that they have been placed under surveillance. The apprehension that the government may be watching is enough to alter individual behaviour and reduce the ability for 'critical subjectivity', which is an essential part of democracy.[37]

The privacy harms of surveillance are further intensified in the age of technology. Technology has enabled and enhanced extensive GPS monitoring, data mining and profiling abilities of the State, coupled with an ease of collection and analysis of metadata.[38] The State's capacity to encroach upon the private sphere has increased the asymmetric power imbalance between the citizens and the State,[39] and this concentration of power is inimical to a constitutional democracy.

Kaul J, in his concurring opinion in *Puttaswamy*, correctly captured the dangers that technology poses to privacy, noting

---

[33] Laurent Sacharoff, 'The Relational Nature of Privacy' (2012) 16(4) Lewis & Clark Law Review 1249, 1282-83; Neil Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review 1934, 1955.

[34] Committee of Experts under the Chairmanship of Justice BN Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) 123.

[35] Richards, 'Dangers of Surveillance' (n 33) 1935, 1957.

[36] See (n 27).

[37] Daniel Solove, 'I've Got Nothing to Hide' (2007) 44 San Diego Law Review 745, 758; Julie Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904, 1912; Richard Clarke et al, 'Liberty and Security in the Changing World' (2013) White House Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies 47.

[38] Christina Moniodis, 'Moving from Nixon to NASA: Privacy's Second Strand - A Right to Informational Privacy' (2012) 15(1) Yale Journal of Law and Technology 139, 154; *Puttaswamy* (n 10) [304].

[39] *Kyllo v United States* 533 US 27, 34 (2001) (US Supreme Court); *Carpenter v United States* No 16-402, 138 S Ct 2206 (2018) 6 (US Supreme Court).

> *The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling and data collection and processing. Surveillance is not new, but technology has permitted surveillance in ways that are unimaginable.*[40]

This echoes the position in other jurisdictions. In the US, for instance, the concurring opinions in *US v Jones*[41] acknowledged that '[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical'.[42] This is because traditional surveillance methods required time and money, were difficult to scale, and had to function on limited police resources. Modern day surveillance techniques, on the other hand, reveal more information, especially when surveillance is carried out over a prolonged time period.[43]

These harms thus recognise the societal interest served by the right to privacy and its importance in a constitutional democracy,[44] and in protecting the rights of the marginalised.[45] They will play an important role when we consider the constitutionality of illegally obtained evidence and lack of judicial oversight over surveillance actions.

B. The Standard for Testing Privacy Violations

Indian courts have long recognised that, in testing the constitutionality of a rights-restricting government measure, a proper balance must be struck between fundamental rights and State action limiting such rights.[46] Striking this balance involved factoring in the 'disproportion of the imposition', and accounting for both the nature of the right and the purpose of the restriction.[47] This was forgotten by Indian courts along the way, as is evident from the judgment in *Maneka Gandhi v Union of India.*[48]

---

[40] *Puttaswamy* (n 10) [585].

[41] 565 US 400 (2012) (Sotomayor J and Alito J concurring) (US Supreme Court).

[42] ibid 963.

[43] ibid 964.

[44] Ruth Gavison, 'Privacy and the Limits of the Law' (1980) 89 Yale Law Journal 421, 455; Chinmayi Arun, 'Paper-Thin Safeguards and Mass Surveillance in India' (2014) 26 National Law School India Rev 104, 114; Kirsty Hughes, 'Mass Surveillance and The European Court of Human Rights' (2018) 6 European Human Rights Law Review 589, 598.

[45] David Gray and Danielle Citron, 'The Right to Quantitative Privacy' (2013) Minnesota Law Review 62, 79.

[46] *Chintaman Rao v State of MP* (1950) SCR 759, 763.

[47] *State of Madras v VG Row* (1952) SCR 597, 607.

[48] (1978) 2 SCR 621, 667-73.

Maneka Gandhi established the idea that the rights protected by the Indian Constitution do not exist in watertight silos, and that a law limiting liberty (Article 21) must also be tested against the guarantee of equality (Article 14) in order to ensure that such law was substantively fair, just and reasonable.[49] However, the decision was somewhat vague on what this really meant. All it told us was that a law limiting liberty must not be arbitrary, fanciful or oppressive in order for it to be reasonable.[50] This was a fairly low bar, which could be satisfied by pointing to a legitimate government objective, since an arbitrary act only suggests 'an absence of any reason whatsoever'.[51]

However, the language of proportionality in Indian constitutional jurisprudence, has now gained traction once again,[52] putting flesh on the bones of the idea that a law must be fair, just and reasonable. *Puttaswamy* and *Aadhaar* have gone some way in lending structure to this strain of proportionality analysis (though some scholars see it as a lost opportunity to articulate a clearer and more stringent test.[53])

In essence, these two cases help us construct a clearer picture of the tests a law must overcome for it to pass muster as fair, just and reasonable. The *Puttaswamy* plurality tells us that the 'procedural and content-based mandate of Article 21'[54] requires the fulfilment of the following criteria to test restraints on privacy:[55]

Legality—The restraint must emanate from a law.

Legitimacy, Suitability and Necessity—The restraint must serve a legitimate State aim or interest and must be necessary in a democratic society.[56] There are actually three steps involved here:

---

[49] ibid 673-674.

[50] ibid.

[51] Tarunabh Khaitan, 'Beyond Reasonableness – A Rigorous Standard of Review for Article 15 Infringement' (2008) 50(2) Journal of Indian Law Institute 177, 191.

[52] *Om Kumar v Union of India* (2001) 2 SCC 386; *Teri Oat Estates v UT Chandigarh* (2004) 2 SCC 130; *Modern Dental College & Research Centre v State of MP* (2016) 7 SCC 353.

[53] Aparna Chandra, 'Proportionality in India: A Bridge to Nowhere?' (2020) 3(2) U of OxHRH J 55.

[54] *Puttaswamy* (n 10) [310] (Chandrachud J).

[55] ibid [310], [325] (Chandrachud J), [638], [639] (Kaul J).

[56] ibid [638] (Kaul J). The standard expounded by Justice Chandrachud in the majority opinion has been fleshed out by Justice Kaul, who sees the prongs of legitimacy and necessity as intrinsically connected. See Gautam Bhatia, 'The Supreme Court's Right to Privacy Judgment – VI: Limitations' (*Indian Constitutional Law and Philosophy*, 1 September 2017) <https://indconlawphil.wordpress.com//?s=right+to+privacy+proportionality+bhatia&search=Go> accessed 25 August 2019.

(i) Assessing the legitimacy of the government's objective.

(ii) Ascertaining that the rights-restraining measure suitably serves the government's objective. There bears a rational relationship to such objective.

(iii) Establishing that such a measure is necessary in a democratic society. This would, ordinarily, place an affirmative burden on the State to establish a minimal impact on individual rights.[57]

Balancing—The incursion into or restriction upon a fundamental right must be proportionate to the need for such interference.

Procedural Safeguards—There must be procedural guarantees in place to check abuse.[58]

Legality emphasises an established principle in Indian constitutional jurisprudence that incursions into fundamental rights must have legislative backing.[59] Legitimacy, Suitability, Necessity and Balancing, together, constitute the proportionality test. The doctrinal source of Procedural Safeguards is unclear, but it would appear, from a reading of decisions rendered by the European Court of Human Rights (ECtHR), that the requirement of such safeguards could possibly can be traced to a positive obligation on the State to safeguard private data, even if a privacy-limiting measure allows the government to access such private information.[60]

This schema was revisited in *Aadhaar*. There was some controversy, in particular, in respect of the necessity limb of the proportionality test, especially the applicability of the 'least intrusive' standard.[61] Sikri J, writing for the majority, articulated the proportionality standard as comprising four components. First, a rights-restricting measure must have a legitimate goal or proper purpose (legitimate goal stage); second, it must be a suitable means of furthering this goal (suitability or rational connection stage); third, there must not be any less restrictive but equally effective alternative (necessity stage); and fourth, the measure must not have a disproportionate

[57] Bhatia, 'Right to Privacy Judgment' (n 56).

[58] *Puttaswamy* (n 10) [311] [314] (Chandrachud J), [638] (Kaul J).

[59] See *State of Madhya Pradesh v Thakur Bharat Singh* [1967] 2 SCR 454; *Bishan Das v State of Punjab* [1962] 2 SCR 69.

[60] *Craxi (No 2) v Italy* (2003) ECHR 25337/94 [73], [74] (European Court of Human Rights).

[61] The State argued that the least intrusive standard was not a part of proportionality, whereas the Petitioners argued that such a standard ensured a minimal invasion of privacy. See *Aadhaar* (n 11) [292] (Sikri J), [816] (Bhushan J), [1261] (Chandrachud J).

impact on the right holder (balancing stage), there should be a proper relation between the importance of achieving the aim and limiting the right.[62] This appears to correspond to the Legitimacy, Suitability, Necessity and Balancing described above, derived from *Puttaswamy*. However, it has been pointed out[63] that *Aadhaar*, instead of insisting on a stricter standard where the State had to demonstrate that there was no less restrictive but equally effective alternative in order to satisfy the necessity limb of the proportionality test, chose to adopt[64] a more forgiving formulation found in the work of Professor David Bilchitz. The *Aadhaar* majority observed

> *First, a range of possible alternatives to the measure employed by the Government must be identified. Secondly, the effectiveness of these measures must be determined individually; the test here is not whether each respective measure realises the governmental objective to the same extent, but rather whether it realises it in a 'real and substantial manner'. Thirdly, the impact of the respective measures on the right at stake must be determined. Finally, an overall judgment must be made as to whether in light of the findings of the previous steps, there exists an alternative which is preferable; and this judgment will go beyond the strict means-ends assessment favoured by Grimm and the German version of the proportionality test; it will also require a form of balancing to be carried out at the necessity stage.*[65]

Therefore, the necessity facet of Legitimacy, Suitability, Necessity now requires

(i) Preparing a menu of alternatives to the Government's proposed measure.

(ii) Assessing the effectiveness of each alternative, asking whether the alternatives achieve the Government's purpose in a 'real and substantial manner'.

---

[62] ibid [319], [494], [511.5].

[63] Mariyam Kamil, 'The Aadhaar Judgment and the Constitution – II: On Proportionality' (*Indian Constitutional Law and Philosophy*, 1 September 2017) <https://indconlawphil.wordpress.com/2018/09/30/the-aadhaar-judgment-and-the-constitution-ii-on-proportionality-guest-post/> accessed 08 November 2019.

[64] *Aadhaar* (n 11) [158] (Sikri J).

[65] ibid [155] (Sikri J).

(iii) Mapping the impact of each alternative on the right in question.

(iv) Carrying out a 'balancing' analysis to decide whether there is a preferable alternative, pointing to the fact that the proposed measure is not, in fact, necessary.[66]

In the next section, we assess the impact of *Puttaswamy* and *Aadhaar* in enumerating the harms of surveillance and in crafting the appropriate judicial review standard and use this to consider whether judicial oversight of surveillance is an imperative under the Indian Constitution.

3. Judicial Oversight Over Surveillance: A Constitutional Imperative Post-Puttaswamy?

While *Puttaswamy* and *Aadhaar* were not directly concerned with the constitutionality of India's surveillance architecture, they offer a clear direction in thinking through the harms of surveillance[67] and in pointing towards the need for judicial oversight over surveillance.

First, we need to understand, as a threshold matter, why judicial oversight is desirable from a structural perspective, in a system committed to the rule of law.

The Indian Supreme Court has held that the guarantee of equality before law under Article 14 of the Constitution is a facet of the rule of law, which requires adjudication of fundamental rights before an independent judicial forum.[68] This is because disputes as to the legality of governmental action should be decided by impartial judges, who are independent of the executive.[69] The absence of accountability in the form of judicial scrutiny, thus, endangers the rule of law, apart from skewing the horizontal separation of powers between the executive and judiciary.

Inter-branch oversight, specifically judicial oversight, over intrusive State action flows from the rule of law requirement. This idea is not unique

[66] This formulation stops short of insisting on the least intrusive alternative, instead prescribing a balancing analysis to arrive at a 'preferable' alternative. Further, another valid criticism is that this judgment provides little guidance either on the balancing stage of the proportionality test (barring a reference to the possibility of adopting 'bright-line rules'), or on the balancing step of the necessity stage. See Kamil (n 63).

[67] Aparna Chandra, 'Privacy and Women's Rights' (2017) 52(51) Economic and Political Weekly 46, 48.

[68] *Union of India v Madras Bar Association* (2010) 11 SCC 1 [101] [102].

[69] ibid.

to India.[70] The ECtHR in *Klass v Germany*[71] stressed that even though courts are not required to substitute the policy assessment of the legislature, and while the threat of terrorism is real, States do not enjoy an 'unlimited discretion to subject persons within their jurisdiction to secret surveillance' and that

> *....The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure.*[72]

The consequence of this dilution of the rule of law, brought about by the absence of judicial oversight, is felt by the individual, and requires to be tested at the level of the impact on individual rights.

A. The Governing Statutory Framework

As mentioned earlier, the surveillance framework in India is regulated by section 5(2) of Telegraph Act 1885 and section 69 of the Information Technology Act 2000 (IT Act 2000) and the accompanying rules framed under these statutes. Under both regimes, the authorising agency which directs the interception, monitoring, decryption of communication is usually the Secretary to the Government of India in the Ministry of Home Affairs at the national level, and the Home Secretary, at the State level.[73] This framework does not provide for judicial oversight prior to the authorisation of surveillance by the executive.

Even at the stage of review, the power to determine whether directions issued by the authorising agency are compliant with the statute is vested entirely in the executive, in the form of a Review Committee. The Review Committee at the Centre comprises of the Cabinet Secretary; the Secretary to the Government of India, Legal Affairs; and Secretary to the

[70] Ann Cavoukian, 'Privacy, Transparency, and the Rule of Law: Critical to Preserving Freedom and Liberty' (2005) 19 National Journal of Constitutional Law 193, 196; Hughes (n 44) 592-93, 596.

[71] (1979-80) 2 EHRR 214 (European Court of Human Rights).

[72] ibid [49], [55].

[73] Indian Telegraph Rules 1951, Rule 419A(1)-(2); The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009, Rule 2(d) read with Rule 2(3).

Government of India, Ministry of Telecommunications.[74] The decision taken by the Review Committee is final and is not subject to any parliamentary or judicial oversight. There is also no requirement to grant a hearing to the proposed surveillance target at any stage.

The first serious challenge to the surveillance framework was decided in 1997, when the constitutionality of section 5(2) of the Telegraph Act was called into question in *PUCL*.[75] It was argued that prior judicial scrutiny of a telephone tapping order was the only way to safeguard privacy rights. However, noting the absence of any statutory provision stipulating judicial oversight, and relying on prevailing English law set out in the Interception of Communications Act 1985, the Supreme Court held that it was 'not possible to provide for prior judicial scrutiny as a procedural safeguard.'[76] The court upheld the constitutionality of the Telegraph Act while issuing a series of guidelines, that eventually led to the insertion of Rule 419A in the Telegraph Rules.[77] These guidelines were meant to act as safeguards against abuse of surveillance powers.[78]

B. Re-Thinking Judicial Oversight after Puttaswamy

Notably, after the judgment in *Puttaswamy*, the constitutionality of the entire surveillance regime (which now includes the IT Act 2000) has been challenged afresh before the Supreme Court.[79] The matter is *sub judice*. One of the grounds for challenge is that lack of prior judicial scrutiny of surveillance actions is unconstitutional.

This argument is premised on the fact that *PUCL* merits reconsideration. First, the constitutionality of Section 5(2) of the Telegraph Act was not 'seriously challenged' in *PUCL*.[80] The Court also did not consider the breadth of the right to privacy under the Indian Constitution or the harms of surveillance in deciding whether judicial oversight was an imperative.[81] After *Puttaswamy*, there is a clearer sense of the impact of

[74] Indian Telegraph Rules 1951, Rule 419A(16) and (17); IT Rules 2009, Rules 2(q) read with Rule 7 and Rule 22.

[75] (1997) 1 SCC 301.

[76] ibid [33]-[34].

[77] Ramachandran (n 4) 111-12.

[78] ibid.

[79] Section 69 of IT Act 2000 and the 2009 Rules 2009 have been challenged in *Internet Freedom Foundation v Union of India,* WP (C) No 44/2019 while Section 5(2) of the Telegraph Act and Rule 419A of the Telegraph Rules have been challenged in *PUCL* (n 12).

[80] *PUCL* (n 12) [27].

[81] ibid [18].

surveillance on privacy. After all, a richer articulation of the right to privacy heightens the quality of justification required for its interference.[82]

Second, *PUCL* merely stated that procedural safeguards must be 'just, fair and reasonable',[83] based on the applicable legal standard at the time, the old *Maneka Gandhi* standard. It has now been urged[84] before the Supreme Court that, after *Puttaswamy* and *Aadhaar*, the question of whether the present surveillance framework passes constitutional muster in the absence of judicial oversight must be answered with reference to the proportionality standard, which provides a workable test for determining whether a law is just, fair and reasonable.

Third, the Court's observations on the absence of judicial scrutiny were based on the submissions of counsel relying on the UK Interception of the Communications Act 1985, which was used to justify safeguards which stopped short of judicial oversight.[85] However, the 1985 Act was subsequently held to be incompatible with the European Convention for Human Rights,[86] and was repealed by the Regulation of Investigatory Powers Act 2000, which contained provisions for judicial oversight. Even the present UK statute, the Investigatory Powers Act 2016, requires prior approval of interception warrants by the Judicial Commissioner to ensure compliance with the proportionality standard.[87]

Highlighting the evolution in privacy law is instrumental in convincing the Supreme Court to rethink its previous pronouncement in *PUCL*. That, however, will not alone be sufficient. In the next section, we explain why the lack of judicial scrutiny over surveillance runs substantively against the grain of the Indian Constitution and fails to satisfy the proportionality standard.

C. Judicial Oversight: A Constitutional Imperative

It is self-evident that surveillance impacts the fundamental right to privacy inherent in Article 21 of the Constitution. The question, however, is whether the present surveillance framework, in the absence of judicial oversight, would survive the applicable standard for testing privacy violations.

---

[82] Hughes (n 44) 597-98.

[83] *PUCL* (n 12) [17] [30].

[84] Indian Telegraph Rules 1951, Rule 419A(1)-(2); IT Rules 2009 Rules 2009, Rule 2(d) read with Rule 2(3).

[85] *PUCL* (n 12) [10] [31]-[34].

[86] *Liberty v United Kingdom* (2009) 48 EHRR 1 [16], [35], [43], [69] (European Court of Human Rights).

[87] Srikrishna Report (n 34) 125-126.

The authorisation of surveillance is backed by law, namely the Telegraph Act 1885 and the IT Act 2000. Therefore, since the requirement of legality is satisfied, we will only consider whether the absence of independent, judicial oversight fails the steps comprising the proportionality test, and whether such a system incorporates adequate safeguards to check abuse.

1. Proportionality Analysis

National security objectives and crime control are legitimate State objectives, according to the *Puttaswamy* judgment itself.[88] Arguably, the government could, in individual cases, justify the rational relationship between surveillance actions and one of these two broad purposes: national security and crime control. This would leave us with the necessity and balancing stages of the proportionality test.

The question, therefore, would be whether exclusive executive review is necessary in a democratic society, and whether exclusive executive control over surveillance has a disproportionate impact on the right holder (whether it fails the balancing test).

The test of necessity would require us to go through the Bilchitz drill prescribed in *Aadhaar*, where we first prepare a list of alternatives, examine their effectiveness, assess their impact on individual rights and then carry out a balancing analysis to arrive at the preferable alternative. Possible alternatives include: (i) *ex ante judicial authorisation and scrutiny*, such as the approval of warrants concerning surveillance by a Judicial Commissioner under the Investigatory Powers Act 2016 in the UK. There would be the additional alternative of such proceedings involving *ex ante* scrutiny being closed to the public, as is the case under the Foreign Intelligence Surveillance Act of 1978 in the US, in cases involving terrorism or espionage; or (ii) *ex post scrutiny*, with individuals being notified after cessation of surveillance.[89]

The impact on fundamental rights is also palpably higher in the absence of judicial scrutiny. In the present system, since aggrieved citizens have no knowledge about being placed under surveillance, even after the completion of surveillance actions, they have no recourse to judicial review under Articles 32 or 226 of the Constitution. Consequently, there is no

[88] *Puttaswamy* (n 10) [311] (Chandrachud J), [639] (Kaul J).

[89] A third system would be one where surveillance evidence is scrutinized in trial, through strict rules of admissibility, but this may by circumvented in cases where material is used for intelligence purposes, as opposed to such material being utilized in trial. See TJ McIntyre, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective' in Martin Scheinin et al (eds), *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar 2016).

occasion for them to seek enforcement of their privacy rights before an independent judicial forum. This undermines the concept of access to justice[90] and procedural due process,[91] which are central to the Indian Constitution. With *ex ante* judicial scrutiny, a judicial body would be tasked with balancing privacy against the executive government's stated objectives in carrying our surveillance, as opposed to this being left to a review committee consisting of executive functionaries. In the case of *ex post* scrutiny, the aggrieved citizen would herself be able to approach a court for redress. Either system is preferable to the status quo, on balance, given that the available alternatives are, on the face of it, both equally efficacious and more respectful of individual rights.

It would follow, therefore, that secret surveillance, which is subject only to executive oversight—as in India—fails the proportionality test.

2. Lack of Procedural Safeguards

The need for judicial oversight has been recognised by the Supreme Court in *Aadhaar*, when it struck down section 33(2) of the Aadhaar Act, which vested the power to authorise disclosure of biometric/demographic information in the interest of national security to the Joint Secretary. The Court ruled that the Joint Secretary was too lowly ranked and that to rule out 'any possible misuse', such authorisation requires 'application of judicial mind for arriving at the conclusion that disclosure of information is in the interest of national security, are prevalent in some jurisdictions' by a judicial officer, who was 'preferably a sitting High Court Judge'.[92]

PUCL held that prior judicial scrutiny was not a necessary procedural safeguard to uphold the constitutionality of section 5(2) of the Telegraph Act 1885.[93] Apart from the fact that *PUCL* requires reconsideration (as discussed above), the current surveillance provisions concentrate disproportionate power in the hands of the executive, without a case-by-case judicial scrutiny to assess whether the proposed surveillance action is compliant with statutory requirements. There is no safeguard against the conflict of interest inherent in the Home Secretary authorising surveillance, whose validity can only be reviewed by her colleagues, who constitute the Review Committee.[94]

Such conflict of interest becomes relevant, for instance, when it comes to the question of identifying cases where material collected in the course of surveillance ought to be destroyed. The Supreme Court's directions in

[90] *Anita Kushwaha v Pushp Sudan* (2016) 8 SCC 509 [31], [33].
[91] *Puttaswamy* (n 10) [280], [291], [449], [450].
[92] *Aadhaar* (n 11) [513.6].
[93] *PUCL* (n 12) [34].
[94] Ramachandran (n 4) 118.

PUCL requires destruction of intercepted material when statutory provisions are violated,[95] and this is now provided for under Rule 419A(17) of the Indian Telegraph Rules 1951. Cross-branch oversight is a more robust mechanism to ensure that this is followed, and to realize the State's positive duty to safeguard an individual's private information in its custody. Given the default rule in India with respect to the admissibility of illegally obtained evidence when relevant, the executive branch (in its prosecuting role) would have a clear incentive to overlook violations and allow retention of illegally intercepted material.

Therefore, safeguarding abuse of power by the executive through judicial oversight is the constitutionally correct safeguard, if the State's positive duty to protect private intercepted material is to be enforced.

The absence of judicial oversight of clandestine government surveillance in India ensures that an accused person discovers the fact of surveillance (if at all) during trial. Even if evidence was collected illegally, it would be admissible in trial. This essentially ensures that the accused has no occasion to ever challenge the illegal or unconstitutional use of state power against them.

4. Puttaswamy *and Evidence Obtained Through Rights Violations*

A. Competing Choices in Criminal Procedure

Recent scholarship[96] examining the confluence between the Constitution of India and the criminal trial process, uses Herbert Packer's opposing 'Crime Control Model', which 'requires that primary attention be paid to the efficiency with which the criminal process operates to screen suspects, determine guilt, and secure appropriate dispositions of persons convicted of crime',[97] and the 'Due Process Model', which focuses on the 'concept of the primacy of the individual and the complementary concept of limitation on official power'.[98] The latter would, according to Packer, 'accept with considerable equanimity a substantial diminution in the

[95] *PUCL* (n 12) [35].

[96] Aparna Chandra and Mrinal Satish, 'Criminal Law and the Constitution' in Sujit Choudhry et al (eds), *The Oxford Handbook of the Indian Constitution* (OUP 2016) 794-95; Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (HarperCollins India 2019) 301-05.

[97] Herbert Packer, 'Two Models of the Criminal Process' (1964) 113 University of Pennsylvania Law Review 1, 10.

[98] ibid 16.

efficiency with which the criminal process operates in the interest of preventing official oppression of the individual'.[99] Developing this idea, Chandra and Satish posit that the liberty perspective (emphasising individuals liberties) and the public order perspective (emphasising social control and security) are 'tendencies, instead of binaries'.[100] They show through in inter se prioritisation when two competing interests are balanced against each other.[101] Put simply, in hard cases involving criminal procedure, the outcome reflects the lens through which the court views the case. Courts adopting the liberty perspective see the legal framework governing the criminal justice system as limiting the power of State to restrict individual liberty, which would include dignity, autonomy and privacy.[102] Conversely, a judge who interprets constitutional rights restrictively, giving the State wide power to determine guilt and punish the guilty, adopts the public order perspective.[103]

We believe that *Puttaswamy* and *Aadhaar* mark an inflection point and present an opportunity for Indian jurisprudence to focus on the liberty perspective, particularly in the treatment of illegally obtained evidence.

B. Crumbling Foundations: The Impact of Puttaswamy *on Illegally Obtained Evidence*

The default rule in India is that evidence obtained by government authorities by illegal means remains admissible where relevant. A review of this line of precedent[104] reveals that this body of law is built on a foundation erected primarily by three previous cases – *MP Sharma*,[105] *RM Malkani v State of Maharashtra*[106] and *Pooran Mal v Director of Inspection (Investigation)*.[107]

The Supreme Court's decision in *State (NCT of Delhi) v Navjot Sandhu*[108] (which cites both *Malkani* and *Pooran Mal*) is direct authority for the proposition that an illegally intercepted telephone conversation is

[99] ibid.
[100] Chandra and Satish (n 96) 795.
[101] ibid.
[102] ibid.
[103] ibid.
[104] *State v NMT Joy Immaculate* (2004) 5 SCC 729 [14], [15.1]; *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600 [154]-[155]; *Umesh Kumar v State of AP* (2013) 10 SCC 591 [35]; *Bharati Tamang v UOI* (2013) 15 SCC 578 [27]-[28]; *Madhu v State of Karnataka* (2014) 12 SCC 419 [23].
[105] *MP Sharma* (n 15).
[106] (1973) 1 SCC 471.
[107] (1974) 1 SCC 345.
[108] (2005) 11 SCC 600 [153]-[155].

admissible as evidence. By analogy, arguably, this would also extend to illegally intercepted electronic communications.

The foundation of this body of law, however, has been hollowed out by *Puttaswamy*. The *Puttaswamy* Court unanimously overruled the decision in *MP Sharma*,[109] which is, in turn, had been relied upon by the Court in *Pooran Mal*.[110] Similarly, *Puttaswamy* explicitly discusses *Malkani* as the jurisprudential progeny[111] of *Kharak Singh*, and then overrules *Kharak Singh* to the extent that it negates the existence of privacy as a constitutionally protected right.[112] Therefore, an important reason for reviewing the default rule in respect of the admissibility of illegal evidence in India is that the precedential basis for this rule has been eroded, which we explore below.

1. *MP Sharma*

The *MP Sharma* decision emerged from an investigation into the affairs of a company whose funds had been misappropriated, with the aid of affiliated entities, in order to defraud its shareholders.[113] The Supreme Court was deciding whether the seizure of incriminatory documentation by law-enforcement authorities from an accused person violated the constitutional guarantee against self-incrimination under Article 20(3) of the Indian Constitution. The Court, in this context, observed

> *A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction.*[114]

There are three distinct ideas here. First, there is an emphasis on the overriding power of the State which includes the search and seizure power of law enforcement authorities. This is clearly a reflection of the public

[109] *Puttaswamy* (n 10) [652.1].
[110] *Pooran Mal* (n 107) [8], [23].
[111] *Puttaswamy* (n 10) [51].
[112] ibid [652.2].
[113] *MP Sharma* (n 15) 1079-81.
[114] ibid 1096-97.

order perspective.[115] Second, the only counterweight to State power is its regulation by law. Finally, the Court refused to recognise the existence of a right to privacy in India, characterising any recognition of this right as the equivalent of artificially grafting the Fourth Amendment of the US Constitution into the Indian Constitution. In other words, the Court failed to locate a textual source for the right to privacy in India as a counterweight to State's overriding power, which is also why it saw statutory prescriptions as the only check on such power.

This is significant, because while *MP Sharma* was not a case dealing directly with the admissibility of illegally obtained evidence, it made an important observation on illegal searches, grounded in the idea that the right to privacy is foreign to the Indian Constitution

> *It is, therefore, impossible to derive from Boyd case [116 US 616], support for the proposition that searches and seizures, in general, are violative of the privilege of protection against self-incrimination. Nor is it possible to import that doctrine with its differentiation between legal and illegal searches into our Constitution because we have nothing in our Constitution corresponding to the Fourth Amendment enabling the courts to import the test of unreasonableness or any analogous criterion for discrimination between legal and illegal searches.*[116]

As per *MP Sharma*, there was no constitutional principle which could be used to classify certain searches as illegal.

Puttaswamy unequivocally strikes down[117] *MP Sharma*, insofar as the latter holds that the right to privacy is not protected by the Constitution. However, the significance of *Puttaswamy* goes far beyond this. First, *Puttaswamy* has displaced the assumption of an overriding power in respect of search and seizure aimed at the protection of social security. Privacy, post-*Puttaswamy*, has been rounded out in a way that provides a significant *constitutional* hurdle for State power to contend with, eviscerating the tacit assumption in *MP Sharma* that the only counterweight to search and seizure powers of the State are those checks and balances introduced by way of *statutory* safeguards. This marks a departure from the public order perspective reflected in *MP Sharma*.

Second, by specifically recognising informational and intellectual privacy, it has negated the finding in *MP Sharma* that the right to privacy

[115] See Bhatia, *Transformative Constitution* (n 96) 307.
[116] *MP Sharma* (n 15) 1092 (emphasis added).
[117] *Puttaswamy* (n 10) [652.1]-[652.2].

is somehow foreign to our Constitution. The Constitution may not speak directly of 'unreasonable searches and seizures', like the Fourth Amendment of the US Constitution, but it does, according to *Puttaswamy*, allows us to 'be secure in [our] persons, houses, papers, and effects'.[118] If a strong conception of privacy as articulated in *Puttaswamy* is a part of the Indian Constitution, then searches in contravention of this right amount to unconstitutional state action. If not, informational and intellectual privacy become meaningless.

2. *Malkani*

MP Sharma is only one part of the troika that forms the foundation of the default rule in India regarding the admissibility of illegally obtained evidence, even though it does not actually deal with the issue head on. The second case in this troika is the 1973 decision in *Malkani*. Chandrachud J, in *Puttaswamy*, states that this case 'followed the same line of reasoning' as *Kharak Singh*.[119] Notably, *Kharak Singh* was set aside in *Puttaswamy*.[120] It would follow, therefore, that a subsequent ruling following *Kharak Singh's* line of reasoning would also implicitly be considered bad law in the future. However, one need not rely on Chandrachud J's observation alone to conclude that *Malkani* is not persuasive in post-*Puttaswamy* India.

The Supreme Court in *Malkani* was dealing with allegations of bribery against the Coroner of Bombay, who contested the admissibility of his conversation recorded with the aid of a device attached to the informant's phone. According to the Coroner, this conversation was illegally obtained in violation of Section 25 of the Indian Telegraph Act 1885.[121] The Court came to the conclusion that fixing a recording instrument to the informant's telephone was not a violation of the Telegraph Act, as it did not amount to damaging, removing, tampering with, or touching any battery, machinery, telegraph line or post for interception of any message within the meaning of the provision.[122] Once it concluded that the evidence was not illegally obtained, the Court need not have made any observation on the admissibility of illegally obtained evidence.

[118] Fourth Amendment of Constitution of United States 1787.

[119] *Puttaswamy* (n 10) [51]. However, *Kharak Singh* (n 16) does not cite *Malkani* (n 106) and Chandrachud J does not explain why there is similarity in reasoning between the two decisions. One clear similarity is that neither locates the right to privacy within Article 21. However, another explanation, provided by Bhatia is that both focused on the 'targeted and specific nature of interception' aimed at law-breakers; Gautam Bhatia, 'State Surveillance and Privacy' (2014) 26(2) National Law School of India Review 127, 133.

[120] *Puttaswamy* (n 10) [652.2].

[121] *Malkani* (n 106) 473-475.

[122] ibid [24].

Instead, the Court deployed a Privy Council ruling[123] to conclude that if evidence is otherwise admissible, the manner of obtaining such evidence is irrelevant.[124] It is important to keep in mind that this observation was made while dealing with evidence collected in violation of a *statutory* provision. The Court had no occasion to deal with evidence derived from a *constitutional* violation, because it did not discern any impact on Article 20(3) and Article 21 rights. According to the Court

> *...The appellant's conversation was voluntary. There was no compulsion. The attaching of the tape-recording instrument was unknown to the appellant. That fact does not render the evidence of conversation inadmissible. The appellant's conversation was not extracted under duress or compulsion...*[125]

This speaks directly to the reliability rationale where lack of voluntariness impacts the quality of the evidence,[126] hampering the court's ability in arriving at the truth. The emphasis on efficiency, without regard for the impact on the individual, squarely reflects the public order perspective. Such a lens views the criminal justice system as a mechanism primed towards social control, achieved through accurate findings of guilt or innocence, followed by the eventual conviction of the guilty. In *Malkani,* the judge was concerned about whether the testimony was 'tainted by coercion or unfairness',[127] which speaks to the quality of the evidence used in arriving at a finding of guilt.

Malkani did not involve telephone tapping or electronic surveillance, where privacy interests are, arguably, heightened. However, permitting the admissibility of evidence based on the fact that a person did not know he was being overheard sounds remarkably like a warrant for carrying out mass surveillance. However, using the individual's lack of awareness of government eavesdropping as a justification for admitting evidence collected through such means, loses sight of the fact that the State must justify, on constitutional principles, its act of eavesdropping, and the consequent violation of privacy even in cases where it attempts to arrive at the truth. A judge analysing this case from the liberty perspective would have mapped the impact of government eavesdropping on the right to privacy.

---

[123] *Kuruma v R* [1955] AC 197.
[124] *Malkani* (n 106) [24]
[125] ibid [30] (emphasis added).
[126] Chandra and Satish (n 96) 803.
[127] *Malkani* (n 106) [29].

By emphasising the liberty perspective, recognising the harms of surveillance, and placing the individual at the centre, *Puttaswamy* requires the State to justify every encroachment into privacy on the touchstone of the proportionality test, even when the information extracted, unknown to the individual concerned, is entirely true. As Kaul J puts it, 'truthful information that breaches privacy may also require protection'.[128] If this principle applies horizontally because there is 'no justification for making all truthful information available to the public',[129] there would, equally, be no reason to give the State unhindered access to conversations and information pertaining to citizens, by allowing it to introduce such information as evidence, without insisting on proper justification.

Malkani then deals with the invocation of the right to privacy as follows

> *...Article 21 was invoked by submitting that the privacy of the appellant's conversation was invaded. Article 21 contemplates procedure established by law with regard to deprivation of life or personal liberty. The telephonic conversation of an innocent citizen will be protected by Courts against wrongful or highhanded interference by tapping the conversation. The protection is not for the guilty citizen against the efforts of the police to vindicate the law and prevent corruption of public servants. It must not be understood that the Courts will tolerate safeguards for the protection of the citizen to be imperilled by permitting the police to proceed by unlawful or irregular methods...*[130]

Malkani does not actually examine the content of personal liberty under Article 21 or clarify whether privacy is a part of liberty. It sidesteps the issue by relying on the 'procedure established by law' formulation of Article 21. Further, as clarified in *Puttaswamy*,[131] the subsequent decision in *Maneka Gandhi*[132] expanded the meaning of the words 'procedure established by law' within Article 21 beyond mere formal adherence to statute, laying down that such procedure must be fair, just and reasonable.[133] Post *Maneka Gandhi*, such statutory procedure must be substantively fair to the target of surveillance. Thus, *Malkani* can no longer be used to justify admissibility of evidence collected in violation of the right

[128] *Puttaswamy* (n 10) [624].
[129] ibid.
[130] *Malkani* (n 106) [31].
[131] *Puttaswamy* (n 10) [19], [22]-[24].
[132] *Maneka Gandhi* (n 48).
[133] ibid [4]-[7].

to privacy because it does not engage with privacy and does not test the substantive fairness of such admissibility.

As an aside, *Malkani* creates a specious distinction between the guilty and the innocent citizen, declaring that innocent citizens somehow enjoy a higher protection. Such a stand is contrary to the text of Article 21 which protects every 'person' and undermines the principle of presumption of innocence which can only be displaced after a trial.[134]

3. *Pooran Mal*

A year after *Malkani*, the Supreme Court in *Pooran Mal*, was grappling with a case of search and seizure under Section 132 of the Income Tax Act 1961. While dealing with a constitutional challenge to this provision, the Court cited *MP Sharma*, drawing on the public order perspective, and stated that '[s]earch and seizure are not a new weapon in the armoury of those whose duty it is to maintain social security in its broadest sense.'[135]

The Appellants sought a Writ of Prohibition in the High Court, restraining the prosecuting agency from using the illegally gathered information as evidence, arguing that the actual search and seizure had violated the statute.[136] In rejecting the Appellant's argument, the High Court had relied on its own earlier decision in *Balwant Singh v Director of Inspection*,[137] where evidence obtained as a result of illegal search and seizure could be used 'subject to the value to be attached to it or its admissibility in accordance with the law relating to evidence'.[138] *Balwant Singh*, however, did not deal with a privacy challenge or, for that matter, any claim under Article 21. In *Pooran Mal*, on the other hand, a claim based on liberty was put forward, without invoking privacy or even Article 21 specifically,[139] as is evident from the following extract

> *Dr. Singhvi who appeared on behalf of the appellants in the two appeals frankly conceded that there was no specific Article of the Constitution prohibiting the admission of evidence obtained in an illegal search and seizure. But he submitted that to admit such evidence is against the spirit of the Constitution which has made our liberties inviolable. In this connection he referred to some*

[134] *Ranjitsing Brahmajeetsing Sharma v State of Maharashtra* (2005) 5 SCC 294.
[135] *Pooran Mal* (n 107) [8].
[136] ibid [20].
[137] AIR 1969 Del 91.
[138] ibid [31].
[139] *Pooran Mal* (n 107) [1] [20].

> *American cases which seem to recognize the validity of his submission.*[140]

In rejecting this, the Court relied on the very paragraph of *MP Sharma*, which speaks of overriding power of the State and suggested that our 'Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy'.[141] The striking down of *MP Sharma*, which is the bedrock supporting *Pooran Mal*, ought to be sufficient to invite the Supreme Court of India to rethink *Pooran Mal*.

However, it may also be useful to refer to the second limb of the rationale in *Pooran Mal*, extracted below

> *Now, if the Evidence Act, 1872 which is a law consolidating, defining and amending the law of evidence, no provision of which is challenged as violating the Constitution — permits relevancy as the only test of admissibility of evidence (See Section 5 of the Act) and, secondly, that Act or any other similar law in force does not exclude relevant evidence on the ground, that it was obtained under an illegal search or seizure, it will be wrong to invoke the supposed spirit of our Constitution for excluding such evidence.*[142]

This rationale cannot, in our view, justify the admissibility of illegally obtained evidence when the illegality in question is a violation of a fundamental right, such as the right to privacy. First, the Indian Evidence Act 1872 is a pre-constitutional legislation, which may be read down in case it conflicts with the Constitution.[143] It cannot therefore be used to get around a privacy claim. However, *Pooran Mal*, as we know, did not recognise privacy in the first place. With *Puttaswamy* locating privacy in the letter and not merely the spirit of the Indian Constitution, the argument in *Pooran Mal* for admitting relevant evidence based on a statutory source stands overridden.

More importantly, however, the Court in *Pooran Mal* was not acting as a criminal court, deciding admissibility of the evidence in question. It was acting as a constitutional court. If it found that a fundamental right had been violated on the ground that the Appellants' liberties had been

[140] ibid [22].
[141] ibid [23].
[142] ibid.
[143] *Anuj Garg v Hotel Association of India* (2008) 3 SCC 1 [7]-[8] [26] [46]; *Navtej Johar v Union of India* (2018) 10 SCC 1 [314] [361] (Nariman J).

encroached upon, nothing in the text of Article 226 of the Indian Constitution prevented the Court from issuing a writ for 'enforcement of any of the rights conferred by Part III'[144] which restored the material seized to the accused and enjoined the prosecuting agency against using this in evidence. It never came to this because the Court refused to recognise the existence of the right to privacy.

As elaborated in Section 2, *Puttaswamy* fleshed out the right to privacy with its liberty-oriented lens. This privacy right, no longer foreign to India, has diluted the public order narrative of the overriding power of the State. As illegal surveillance would trigger a privacy interest, the time is ripe for a re-examination of the default rule in India with respect to the admissibility of illegally obtained evidence. In the next subsection, we make a beginning by analysing a narrower claim, namely that evidence obtained from surveillance carried out in violation of the right to privacy must be excluded and a constitutional court must act to restore such information to the target of surveillance, while enjoining the State against using such evidence in trial.

C. New Directions: An Exclusionary Rule for Evidence Obtained in Violation of the Right to Privacy

If the default admissibility rule is to be re-examined, as we have suggested, it will have to be tested in a constitutional court. The affected person undergoing trial will have to seek a writ remedy for enforcement of her right to privacy, seeking restoration of the status quo through return and/or destruction of evidence collected in violation of such right and prohibiting the prosecuting agency from using this evidence in trial.

There will, possibly, be an additional facet concerning Section 5 of the Indian Evidence Act 1872, often identified as the statutory source for the rule that illegally collected evidence is admissible.[145] The State is likely to urge that it has the right to utilise such evidence in trial, if relevant.

In the absence of a constitutional counterweight to the overriding power of the State in respect of search and seizure, litigants were, so far, grasping at straws in locating a basis for an exclusionary rule within the fundamental rights enumerated in the Indian Constitution. Some invoked Article 19(1)(f), which prior to its deletion in 1978[146] protected the right to property. To this, courts simply stated that this right, at best, entitled

[144] Article 226, Constitution of India 1950.
[145] *Pooran Mal* (n 107) [23]-[24]
[146] Constitution (Forty Fourth) Amendment Act 1978.

restoration of the seized property, but did not preclude the use of evidence in the course of trial.[147] Others invoked Article 20(3), only to run into the counter-argument that this provision would not be triggered in the absence of compulsion.[148] In dealing with Article 21, courts simply denied the existence of any right to privacy, precluding any examination of whether the enforcement of this right led to exclusion of illegal evidence.[149] This situation has prevented Indian courts from distinguishing between evidence collected merely in violation of statute, as opposed to evidence gathered in violation of an individual's fundamental rights.

However, the law which has evolved separately in respect of Article 20(3), which bars admissibility of compelled statements, would lead us to believe that evidence obtained in violation of a fundamental right is excluded from use in trial. Precedent is clear in excluding evidence obtained through testimonial compulsion.[150]

Notably, the text of Article 20(3), which states that '[n]o person accused of any offence shall be compelled to be a witness against himself', speaks directly to the right of an accused being tried for an offence. The text of Article 21 does not immediately point us to the exclusion of tainted evidence obtained in violation of this provision. *Puttaswamy*, however, has given us the vocabulary to articulate the breadth and depth of the right to privacy contained within Article 21, while *Aadhaar* has taken us some way towards crafting the appropriate test for assessing its violations.

Puttaswamy's strong conception of privacy establishes beyond doubt that surveillance impacts privacy, a facet of personal liberty under Article 21. The text of Article 21 permits deprivations of liberty only through procedures established by law.[151] Logically, therefore, if statutory provisions circumscribing the power of the State to carry out surveillance constitute the procedure established by law, the violation of such laws would, necessarily, engage Article 21. Put another way, State action which violates statutory prescription would fail the legality limb of the proportionality test, which requires the curtailment of privacy only under a regime of law.[152]

Restoring the status quo is the appropriate way to enforce the right to privacy. This is evident if we dig deeper into the competing interests at play in conversations surrounding illegal evidence. Some jurisdictions have

[147] *Balwant Singh* (n 137) [32]

[148] *Malkani* (n 106) [30]-[31].

[149] *Pooran Mal* (n 107) [22].

[150] *State of Bombay v Kathi Kalu Oghad* AIR 1961 SC 1808; *Selvi v State of Karnataka* (2010) 7 SCC 263 [134-135]. See Chandra and Satish (n 96) 804.

[151] *Maneka Gandhi* (n 48) [4]-[7]; Abhinav Chandrachud, 'Due Process' in Sujit Choudhry et al (eds), *The Oxford Handbook of the Indian Constitution* (OUP 2016) 794-795; Bhatia, *Transformative Constitution* (n 96) 783-785.

[152] *Puttaswamy* (n 10) [313].

focused the conversation on deterring violations by law enforcement[153] and protecting the integrity of the judicial system.[154] However, this arguably dilutes the remedy, leaving ample room for judicial discretion, where the judge is likely to emphasise individual rights or State interests based on whether she subscribes to the liberty or public order perspective. The integrity of the judicial system may be seen to be served by exclusion of evidence obtained through unconstitutional means. However, its meaning may equally be moulded to emphasise that judicial integrity is served by utilising probative evidence and convicting the guilty.[155] Similarly, deterrence comes up against the difficulties[156] of measuring 'incremental deterrent effect'[157] and balancing this against the government interest in crime control where the probative value of evidence is high.[158]

In the end, the question of excluding evidence gathered by the State in violation of the fundamental right to privacy can only be answered with reference to two core competing interests, namely the insistence on individual liberties underlying the liberty perspective and the State's interest in crime control which forms the core of the public order perspective.

The insistence on individual liberty as the underlying principle justifying the exclusionary rule is not a novel idea. In *Weeks v US*,[159] the US Supreme Court, while acknowledging the State interest underlying the conviction of the guilty, clarified that this cannot undermine the 'great principles established be years of endeavour and suffering which have resulted in their embodiment in the fundamental law of the land'.[160] Later, in *Mapp v Ohio*,[161] Clark J refused to let the right to privacy 'remain an empty promise' which was 'revocable at the whim of any police officer',[162] while holding that the exclusionary rule grounded in the Fourth Amendment's guarantee of privacy was applicable to the States by virtue of the Due Process Clause of the Fourteenth Amendment of the US Constitution.

Similarly, the law in Ireland recognizes the distinction between illegally obtained evidence and evidence obtained as a result of an unconstitutional

---

[153] *Wolf v Colorado* 338 US 25, 31 (1949) (US Supreme Court).

[154] Section 24(2) of the Canadian Charter of Rights and Freedoms; *Bunning v Cross* (1978) 141 CLR 54, 77-8 (High Court of Australia).

[155] Robert Bloom and Erin Dewey, 'When Rights Become Empty Promises: Promoting an Exclusionary Rule that Vindicates Personal Rights' (2011) 46 Irish Jurist 38, 70.

[156] ibid 69.

[157] *US v Calandra* 414 US 338, 354 (1974) (US Supreme Court).

[158] Bloom and Dewey (n 155) 69.

[159] 232 US 383 (1961) (US Supreme Court).

[160] ibid 393.

[161] 367 US 643 (1961) (US Supreme Court).

[162] ibid. 660.

seizure.[163] As a result of *People (DPP) v Kenny*,[164] the law moved towards a strong exclusionary rule where evidence collected while transgressing constitutional rights is admissible only if such transgression is unintentional or accidental, or where a Court is satisfied that there are 'extraordinary excusing circumstances'.[165] Finlay CJ was emphatic in his insistence on upholding constitutional rights when he said

> *The detection of crime and the conviction of guilty persons, no matter how important they may be in relation to the ordering of society, cannot, however, in my view, outweigh the unambiguously expressed constitutional obligation 'as far as practicable to defend and vindicate the personal rights of the citizen.'*[166]

Some may believe that Finlay CJ's words overstate the proposition. Surely, convictions of guilty persons, especially when it comes to serious crimes, would justify the introduction of probative evidence into trial, even if law enforcement authorities violate the rights of the accused in the process? *Puttaswamy*, however, reminds us that constitutional rights are not bounties conferred by the State and, more fundamentally, that the rule of law 'imposes restraints upon the powers vested in the modern State when it deals with the liberties of the individual'.[167] This points to the principle of justification of every exercise of State power if, indeed, the adoption of the Indian Constitution marks a point of 'transformation from a culture of authority to a culture of justification'.[168]

In short, the writ of prohibition enjoining the prosecuting agency against using illegally collected evidence in trial would be justified on the basis that this is the valid constitutional remedy for enforcement of the right to privacy under Articles 32 and 226 of the Constitution of India, thus restoring the status quo ante.

This approach, focusing on the enforcement of the right to privacy, violated at the point of unconstitutional surveillance, may be met with the response that, in fact, privacy is not absolute and that focusing the challenge on the illegal surveillance is misplaced. The State would likely argue that that this case is actually about whether the default rule in India, allowing relevant evidence regardless of the legality of its collection, is a constitutionally permissible deprivation of the right to privacy. This is

[163] *People (AG) v O'Brien* [1965] IR 142, 168 (Walsh J) (Irish Supreme Court).
[164] [1990] 2 IR 110, 134 (Irish Supreme Court).
[165] ibid 134.
[166] ibid.
[167] *Puttaswamy* (n 10) [136] (Chandrachud J).
[168] Bhatia, *Transformative Constitution* (n 96) 294.

where the second limb of the challenge comes in; the reading down of Section 5 of the Indian Evidence Act 1872.

The admissibility of illegal evidence under Indian law does not flow from a statutory or constitutional provision mandating such admissibility. It is, rather, the absence of any provision to the contrary,[169] combined with the adoption of English precedents that has ossified this rule.[170] If, indeed, the Indian Constitution is transformative in its vision,[171] it may finally be time to re-examine this rule, with the aid of *Puttaswamy* and *Aadhaar*.

The Bombay High Court, in a recent judgment has, in fact, seized this opportunity. In a case of illegal surveillance violating section 5(2) of The Telegraph Act 1885, the Court directed destruction of the intercepted material, and, while doing so, dealt with the State's argument regarding admissibility of illegally intercepted material using sound constitutional logic.[172] First, the Court pointed out that *PUCL*, which has been cited with approval in *Puttaswamy*, mandates the destruction of illegally collected evidence. Second, such violation impacts the right to privacy located in Article 21 of the Constitution. The Court finally declared that to ignore fundamental rights and to allow such evidence into trial would set fundamental rights as naught. The Court held

> *To declare that dehorse (sic.) the fundamental rights, in the administration of criminal law, the ends would justify the means would amount to declaring the Government authorities may violate any directions of the Supreme Court or mandatory statutory rules in order to secure evidence against the citizens. It would lead to manifest arbitrariness and would promote the scant regard to the procedure and fundamental rights of the citizens, and law laid down by the Apex Court.*[173]

This goes beyond making the obvious point that mandatory destruction of illegally intercepted material, as per *PUCL*, amounts to an implicit reading down of Section 5 of the Indian Evidence Act 1872 and a consequent dilution of the default rule allowing illegal evidence into trials. In creating a distinction between illegally collected evidence resulting from

[169] *Pooran Mal* (n 107) [23].
[170] ibid [24]; *Malkani* (n 106) [24].
[171] *Navtej Johar* (n 143) [107]-[111], [122] (Misra J); *Indian Young Lawyers Association v State of Kerala* (2018) SCC Online SC 1690 [179]-[181], [248]-[251] (Chandrachud J).
[172] *Vinit Kumar v Central Bureau of Investigation* (2019) SCC Online Bom 3155 [42].
[173] ibid.

minor or venial breaches of statute,[174] and evidence collected in violation of constitution provisions,[175] and in insisting that the ends cannot justify unconstitutional means of achieving such government objectives, the Bombay High Court has reaffirmed the liberty perspective. It has emphatically underscored the importance of individual rights in constitutional adjudication, taking over where *Puttaswamy* left off.

5. Conclusion

Puttaswamy was not a surveillance case. What it gave India, however, is a tapestry of ideas explaining the multiple dimensions of privacy in a way that engaged directly with the impact of surveillance. Along with *Aadhaar*, it provides a framework for testing the existing system of laws governing surveillance.

This system of laws in India today allows the State to ignore individual liberties with impunity. Exclusive executive control over secret surveillance, absent *ex ante* or *ex post* judicial oversight, denies due process. If surveillance culminates in trial, courts are made complicit in such violations by admitting the evidence emerging from such unconstitutional surveillance based on the default admissibility rule. This gives 'unlimited discretion' to the government in matters of surveillance, and this would lead to 'undermining or even destroying democracy on the ground of defending it'.[176]

With a strong conception of privacy focused on individual liberty after *Puttaswamy*, we have tried to show that there is now a starting point for insisting on judicial oversight and an exclusionary rule restricting the admissibility of evidence obtained in violation of privacy rights. These cases allow us to bring the focus back to the liberty perspective, because rights, fundamentally, imply that the State must justify each incursion even at the cost of efficiency.[177]

[174] Courts can subsequently carve out carefully crafted exceptions for minor violations. One such exception, akin to Section 465 of the Code of Criminal Procedure 1973, could be that a mere 'error, omission or irregularity' would not lead to reversing a conviction unless a 'failure of justice' is occasioned thereby.

[175] Bhatia, *Transformative Constitution* (n 96) 323.

[176] *Klass* (n 71) [49].

[177] Carol Steiker, 'Second Thoughts About First Principles' (1994) 107 Harvard Law Review 820, 820.